Инструкция по настройке VPN-подключений

Оглавление

Создание подключения в ОС Windows 10/11	2
Создание подключения с использованием командной строки PowerShell	2
Создание подключения с использованием графического интерфейса системы	4
Создание подключения в OC Windows 7	6
Создание подключения в OC Linux (Ubuntu)	11
Создание подключения на Android смартфонах	12
Создание подключения на iPhone	13
Создание подключения в ОС Мас OS	14

Создание подключения в ОС Windows 10/11

Создание подключения с использованием командной строки PowerShell

1. Для настройки VPN-подключения с использованием командной строки PowerShell нажмите правой кнопкой мыши на иконке меню Пуск и выберете Windows PowerShell (Терминал)



2. Скопируйте и вставьте в открывшееся окно указанную ниже команду для создания VPNподключения и нажмите Enter

Add-VpnConnection -Force -Name "VPN-LIB KPFU" `

-TunnelType IKEv2 ` -ServerAddress vpn-lib.kpfu.ru ` -AuthenticationMethod EAP ` -EncryptionLevel "Required" ` -RememberCredential

🔀 Windows PowerShell



3. В случае успешного выполнения команды, в меню **Сеть** в системном трее появится созданное VPN-подключение



4. Нажмите **Подключиться** и в окне **Безопасность Windows** введите доменное имя пользователя и пароль, и нажмите **ОК**

타.kpfu.ru Подключено	Безопасность Windows × Войти
УРN-LIB KPFU Подключиться	Имя пользователя Пароль Домен:
Параметры сети и Интернет Изменение параметров, таких как установление для подключения значения "лимитное".	Неверное имя пользователя или пароль. ОК Отмена

Создание подключения с использованием графического интерфейса системы

1. Нажмите на значок Сеть в системном трее и откройте Параметры сети и Интернет



2. В открывшемся окне слева в меню выберете пункт VPN и нажмите Добавить VPNподключение

Параметры	
Павная	VPN
Найти параметр \wp	+ Добавить VPN-подключение
Сеть и Интернет	
🕭 Состояние	Дополнительные параметры Разрешить VPN в сетях с лимитным тарифным планом
문 Ethernet	Вкл.
🛱 Набор номера	Разрешить VPN в роуминге Вкл.
% VPN	
Прокси-сервер	

- 3. Заполните поля:
 - Поставщик услуг VPN Windows (встроенные);
 - Имя подключения любое название, например VPN-LIB KPFU;
 - Имя или адрес сервера vpn-lib.kpfu.ru;
 - Тип VPN IKEv2;
 - Тип данных для входа Имя пользователя и пароль;
 - Имя пользователя доменное имя пользователя;
 - Пароль пароль пользователя.

и нажмите Сохранить

Изменение VPN-подключения	
Эти изменения вступят в силу при следующем подключе	ении
Имя подключения	
VPN-LIB KPFU	
Имя или адрес сервера	
vpn-lib.kpfu.ru ×	
Тип VPN	
IKEv2 V	
T	
тип данных для входа	
Имя пользователя (необязательно)	
Пароль (необязательно)	
🗸 Запомнить мои данные для входа	

4. В меню Сеть в системном трее появится созданное VPN-подключение «VPN-LIB KPFU»



Создание подключения в ОС Windows 7

Перед настройкой подключения по протоколу IKEv2 необходимо убедиться в наличии корневого сертификата ISRG Root X1.

1. Откройте оснастку «Сертификаты». Для этого нажмите кнопку «Пуск», в поле Поиск введите certmgr.msc и нажмите Enter.



2. В меню «Действие» выберете «Поиск сертификатов»

Cep 5	Все задачи	13.	
			ческого хранилища
	Обновить Экспортировать списо	к	нные корневые центры сертификации тельные отношения в предприятии
 Дов Сер Сто Дов Зап Дов 	еренные издатели тификаты, к которь ронние корневые це еренные лица росы заявок на серт еренные корневые с	Объект Довере Сертиф Сторон Довере Запрос Довере	⁴ пользователя Active Directory нные издатели фикаты, к которым нет доверия нние корневые центры сертификации енные лица ы заявок на сертификат енные корневые сертификаты смарт-карты

3. Введите в поле «Содержит» ISRG и нажмите «Найти»

Поиск сертифика	тов	×
Файл Правка В	ид Справка	
Искать в: Все :	кранилища сертификатов	
Содержит:	ISRG	Найти
Искать в поле:	Кем выдан	Остановить
		Новый поиск
Подробнее о <u>по</u>	иске сертификатов	2

4. Если поиск дал результат, то можно переходить непосредственно к этапу настройки подключения

	катов					<u>,</u>
Фаил Правка	Вид Справк	a				
Искать в: Во	е хранилища с	ертификато	в			•
Содержит:	ISRG					Найти
Искать в поле	Кем выдан	8			•	Остановить
						Новый поиск
Подробнее о ј	поиске сертиф	икатов				
Подробнее о ј	поиске сертиф	икатов				
Подробнее о ј Кому выдан	поиске сертиф	<u>икатов</u> Срок дей	Назначения	Имя	Найдено хранилище в	
Подробнее о Кому выдан	поиске сертиф Кем выдан ISRG Root X1	<u>икатов</u> Срок дей 04.06.2035	Назначения Проверка подлинн	Имя ISRG Root X1	Найдено хранилище в Сторонние корневые центр	ертификации
Подробнее о <u>Кому выдан</u>	поиске сертиф Кем выдан ISRG Root X1 ISRG Root X1	икатов Срок дей 04.06.2035 04.06.2035	Назначения Проверка подлинн Проверка подлинн	Имя ISRG RootX1 ISRG RootX1	Найдено хранилище в Сторонние корневые центр Доверенные корневые цент	ертификации гры сертификации
Подробнее о <u>кому выдан</u>	поиске сертиф Кем выдан ISRG Root X1 ISRG Root X1	икатов Срок дей 04.06.2035 04.06.2035	Назначения Проверка подлинн Проверка подлинн	Имя ISRG RootX1 ISRG RootX1	Найдено хранилище в Сторонние корневые центр Доверенные корневые цент	СС ы сертификации гры сертификаци
Подробнее о <u>Кому выдан</u>	<mark>Кем выдан</mark> ISRG Root X1 ISRG Root X1	икатов Срок дей 04.06.2035 04.06.2035	Назначения Проверка подлинн Проверка подлинн	Имя ISRG Root X1 ISRG Root X1	Найдено хранилище в Сторонние корневые центр Доверенные корневые цент	то сертификации пры сертификации
Подробнее о Кому выдан ISRG Root X1	поиске сертиф Кем выдан ISRG RootX1 ISRG RootX1	икатов Срок дей 04.06.2035 04.06.2035	Назначения Проверка подлинн Проверка подлинн	Имя ISRG RootX1 ISRG RootX1	Найдено хранилище в Сторонние корневые центр Доверенные корневые цент	ЕСС ны сертификации гры сертификаци
Подробнее о у Кому выдан GilSRG RootX1 GilSRG RootX1	поиске сертиф Кем выдан ISRG RootX1 ISRG RootX1	икатов Срок дей 04.06.2035 04.06.2035	Назначения Проверка подлинн Проверка подлинн	Имя ISRG RootX1 ISRG RootX1	Найдено хранилище в Сторонние корневые центр Доверенные корневые цент	ССР ны сертификации гры сертификаци

- 5. Если сертификат отсутствует, то скачайте корневой сертификат по ссылке <u>https://letsencrypt.org/certs/isrgrootx1.der</u>
- 6. Откройте скачанный сертификат и установите его

🙀 Сведени	я о сертификате	
Этот сертифика	ат предназначается для:	
• Подтвержи	дает удаленному компьютеру идентификац	ию
• Обеспечие	пьютера зает получение идентификации от удаленно	ого
компьютера		
(ому выдан:	ISRG Root X1	
Кем выдан:	ISRG Root X1	
Действите	лен с 04.06.2015 по 04.06.2035	
Устано	вить сертификат Заявление постав	ци
poonee o ceprind	икатах •	

 В мастере импорта сертификатов нажмите «Далее». На странице выбора хранилища сертификатов выберете «Автоматически выбрать хранилище на основе типа сертификата» и нажмите «Далее»

Хранилиша сертификатов - это об	DIACTH CHCTEMELE KOTODEN IDONSBOAHTCH
хранение сертификатов.	ласти системы в которых производится
Выбор хранилища может быть пр можно указать размещение серти	оизведен Windows автоматически, или же фиката вручную.
📀 Автоматически выбрать хр	анилище на основе типа сертификата
О Поместить все сертификат	ы в следующее хранилище
Хранилище сертификатов:	
	<u>О</u> бзор

8. Откройте Центр управления сетями и общим доступом



Q

10. Нажмите Подключение к рабочему месту

Свойства обозревателя

Устранение неполадок

ыбері	ите вариант подключения	
4	Подключение к Интернету Беспроводное, скоростное или телефонное подключение к Интернету.	
2	Создание и настройка новой сети Настройка нового маршрутизатора или точки доступа.	
•	Подключение к рабочему месту Настройка телефонного или VPN-подключения к рабочему месту.	
٩	Настройка телефонного подключения Подключение к Интернету через телефонную сеть.	
*	Подключение к личной локальной сети Bluetooth (PAN) Подключение к устройству или сети с помощью Bluetooth.	

- 11. Нажмите Использовать мое подключение к интернету (VPN) и заполните следующие поля:
 - Интернет-адрес vpn-lib.kpfu.ru; •
 - Имя местоназначения любое название, например VPN-LIB KPFU. •

Установите флаг в пункте **Не подключаться сейчас, только выполнить установку для** подключения в будущем

🚱 🌆 Подключение к рабочему месту				
Введите Интернета-	адрес для подключения			
Этот адрес можно получи	ть у сетевого администратора.			
	Пример: Contoso.com дибо 157.54.0.1. дибо 3ffe:1234-			
интернете-адрес.	[hipmicpi conconcent since 15/15/161 since siteries in			
Имя местоназначения:	VPN			
_				
🔲 Использовать смар	эт-карту			
💡 📃 Разрешить исполы	зовать это подключение другим пользователям			
Этот параметр позе компьютеру, испол	золяет любому пользователю, имеющему доступ к этому пьзовать это полключение.			
сомпьютеру, использовать это подключение.				
📝 Не подключаться сейчас, только выполнить установку для подключения в будущем				
	Далее Отмена			

- 12. В окне Введите имя пользователя и пароль заполните соответствующие поля:
 - Пользователь доменное имя пользователя;
 - Пароль пароль пользователя.

Нажмите Создать, далее Закрыть.

13. В окне **Центр управления сетями и общим доступом**, выберите в левом верхнем углу Изменение параметров адаптера

🔾 🗸 🖓 « Сеть и Ин 🕨 I	Центр управления сетями и общим доступом	 Ч Поиск в панели управления
Панель управления - домашняя страница Изменение параметров	(зтот компьютер) Сеть Сеть	Просмотр полной карты ^
адаптера Изменить дополнительные параметры общего доступа	Гросмотр активных сетеи Сеть Домашняя сеть	Тип доступа: Интернет Подключения: Подключение по локальной сети
	Изменение сетевых параметров	
	Настройка нового подключения ил Настройка беспроводного, широко VPN-подключения или же настрой	и сети ополосного, модемного, прямого или ка маршрутизатора или точки доступа.
	Подключиться к сети Подключение или повторное подкл модемному сетевому соединению	лючение к беспроводному, проводному, или подключение к VPN.
	Выбор домашней группы и параме Доступ к файлам и принтерам, расі	тров общего доступа положенным на других сетевых компьютерах, или
См. также	изменение параметров общего дос	тупа.
Брандмауэр Windows Домашняя группа Свойства обозревателя	Устранение неполадок Диагностика и исправление сетевы исправлении.	х проблем или получение сведений об
		-

- 14. Нажмите правой кнопкой мыши на созданное VPN-подключение, выберите Свойства
- 15. На вкладке Безопасность установите следующие значения:
 - Тип VPN IKEv2;
 - Шифрование данных обязательное (отключиться, если нет шифрования)
 - Протокол расширенной проверки подлинности (EAP) Microsoft: Защищённый пароль (EAP-MSCHAP v2)

Общие Параметры Безопасно Тип VPN: [IKEv2 Шифрование данных: обязательное (отключиться, ес.	ость Сеть Доступ Дополнительные параметры ли нет шифрования)	
Тип VPN: IKEv2 Шифрование данных: обязательное (отключиться, ес.	Дополнительные параметры ли нет шифрования)	
ІКЕv2 Шифрование данных: обязательное (отключиться, есс	Дополнительные параметры ли нет шифрования)	
Шифрование данных: обязательное (отключиться, ес.	Дополнительные параметры ли нет шифрования)	
обязательное (отключиться, ес.	сли нет шифрования)	
		r
 Протокол расширенной про Місгозоft: Защищенный пар 	верки подлинности (EAP) роль (EAP-MSCHAP v2) (ш 🔻	
Использовать сертификать	и компьютеров	
<u>`</u>		_

- 16. Нажмите **ОК** для сохранения настроек
- 17. Нажмите на значок **Сеть** в системном трее, выберете созданное VPN-подключение и нажмите **Подключить**

Создание подключения в ОС Linux (Ubuntu)

- 1. Для создания VPN-подключения на OC Ubuntu, необходимо предварительно запустить **Терминал** и установить необходимые пакеты, выполнив команду sudo apt install -y network-manager-strongswan libcharon-extra-plugins libstrongswan-extra-plugins
- 2. После установки пакетов перейдите в Настройки -> Сеть и нажмите + напротив меню VPN

8

Q Настройки Ξ	Сеть	- 0
😚 Сеть		
Bluetooth	Ethernet (eth0)	+
📮 Фон	10000 Мбит/с	
😰 Внешний вид	Ethernet (eth1)	+
Ф Уведомления	Подключено - 10000 Мбит/с	
О Поиск		
III Приложения >	VPN	+
🔒 Конфиденциальность 🛛 👌	Не настроено	
Сетевые учётные записи		
🐇 Общий доступ	Сетевой прокси Выклю	чено 🔘
Л Звук		

3. В появившемся окне выберите IPsec/IKEv2 (strongswan)

Отменить	Добавить VPN
Layer 2 Tunnelin Совместим с серв	ig Protocol (L2TP) ерами Microsoft и другими серверами L2TP VPN.
OpenVPN	
Совместим с серв	ером OpenVPN.
Туннельный пр	оотокол типа точка-точка (РРТР)
Совместим с серв	ерами Microsoft и другими серверами PPTP VPN.
Туннельный пр	оотокол типа точка-точка (SSTP)
Совместим с серв	ерами Microsoft и другими серверами SSTP VPN.
IPsec/IKEv2 (str	ongswan)
IPsec with the IKEv	2 key exchange protocol.
Импортироват	ь из файла

- 4. В разделе Идентификация и заполните следующие поля:
 - Название любое название, например VPN-LIB KPFU;
 - Address vpn-lib.kpfu.ru;
 - Authentication EAP;
 - Username доменное имя пользователя;
 - Password пароль пользователя (если поле ввода пароля неактивно, нажмите ? и выберете пункт Запомнить пароль для этого пользователя);
 - Установите флаг Request an inner IP address.
- 5. Нажмите Добавить для сохранения настроек

Создание подключения на Android смартфонах

- 1. Для создания VPN-подключения на смартфоне под управлением OC Android, перейдите в раздел Настройки → Wi-Fi и сеть → VPN (У разных производителей смартфонов могут отличаться названия пунктов меню, при необходимости можно воспользоваться стройкой поиска по настройкам).
- 2. Нажмите Добавить профиль VPN
- 3. Заполните следующие поля:

Изменение профиля	VPN
Название	
Тип	
IKEv2/IPSec MSCHA	-
Адрес сервера	
Идентификатор IPSec	
(не используется)	
Сертификат ЦС IPSec	
(не проверять серв	•
Сертификат сервера IPSec	
(получено с сервер	•
Дополнительные параме	тры
Имя пользователя	
Пароль	
Отмена	

- Название любое название, например VPN-LIB KPFU;
- Тип IKEv2/IPSec MSCHAPv2;
- Адрес сервера vpn-lib.kpfu.ru;
- Идентификатор IPSec доменное имя пользователя;
- Сертификат ЦС IPSec не проверять сервер;
- Сертификат сервера получено от сервера;
- Имя пользователя доменное имя пользователя;
- Пароль пароль пользователя.

Создание подключения на iPhone

- 1. Для создания VPN-подключения на смартфонах iPhone, перейдите в раздел Настройки → Основные → VPN
- 2. Нажмите **Добавить конфигурацию VPN**

10:04		ati LTE 💽
🗸 Основные	VPN	
Добавить конфи	гурацию VPN	

3. Выберите тип подключения IKEv2 и заполните следующие поля:

Отменить	Настройка	Готово
Тип		IKEv2 >
Описание об	бязательно	
Сервер	бязательно	
Удаленный ID	обязательно	
Локальный ID		
Алтентифика	ина Имал	ORESORSTERR)
Имя пользова	ателя обязательно	
Пароль ст	прашивать всегда	
ПРОКСИ		
Выкл.	Вручную	Авто
• Описа		

- Описание любое название, например VPN-LIB KPFU;
- Сервер vpn-lib.kpfu.ru;
- Удаленный ID vpn-lib.kpfu.ru;
- Имя пользователя доменное имя пользователя;
- Пароль пароль пользователя.

Создание подключения в ОС Mac OS

- 1. Для создания VPN-подключения на устройствах по управлением ОС Mac OS перейдите в раздел Системные настройки → Сеть
- 2. Нажмите Добавить в левом нижнем углу
- 3. В появившемся окне заполните поля:

Интерфейс:	VPN		0
Тип VPN:	IKEv2		0
Имя службы:	VPN		
		Отменить	Созлать

- Интерфейс VPN;
- Тип VPN IKEv2;
- Имя службы любое название, например VPN-LIB KPFU.

4. Нажмите Создать;

5. Установите параметры подключения:

Подключать по запросу
Настройки аутентификации
Подключить
РN в строке меню Дополнительно ?
Ассистент Вернуть Применить

- Адрес сервера vpn-lib.kpfu.ru;
- Удалённый ID vpn-lib.kpfu.ru.
- 6. Выберите Настройки аутентификации:

Имя пользователя	0
Імя пользователя:	
Пароль:	

- Имя пользователя доменное имя пользователя;
- Пароль пароль пользователя.
- 7. Нажмите ОК;
- 8. Поставьте флаг в пункте Показывать статус VPN в строке меню и нажмите Применить.